S99R1277 U.S.00
#4

JC568 U.S. PTO
09/442727

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１１月１９日

出 願 番 号
Application Number: 平成１０年特許願第３２９９７３号

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年 ９月２４日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

【書類名】　特許願

【整理番号】　9800713305

【提出日】　平成10年11月19日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 29/00

【発明の名称】　信号処理回路

【請求項の数】　8

【発明者】

【住所又は居所】　神奈川県横浜市保土ヶ谷区神戸町１３４番地　ソニー・エルエスアイ・デザイン株式会社内

【氏名】　佐藤　貞治

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100094053

【弁理士】

【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　信号処理回路

【特許請求の範囲】

【請求項１】　送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、

送信すべきデータを所定の暗号モードで暗号化し、暗号化情報とともに出力する暗号処理回路と、

暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路と

を有する信号処理回路。

【請求項２】　上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する

請求項１記載の信号処理回路。

【請求項３】　送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、

少なくとも一つの暗号モード情報が設定される保持手段と、

送信データを暗号化すべきモードを指定する制御手段と、

上記制御手段で指定された暗号モード情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力する暗号エンジン回路とを有する暗号処理回路と、

暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回

路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路と

を有する信号処理回路。

【請求項４】　上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する

請求項３記載の信号処理回路。

【請求項５】　送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、

記憶手段と、

少なくとも一つの暗号モード情報が設定される保持手段と、

送信データを暗号化すべきモードを指定する制御手段と、

上記制御手段で指定された暗号モード情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力する暗号エンジン回路とを有する暗号処理回路と、

受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第１の送信回路と、

上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインタフェースバスに送信し、かつ、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する第２の送信回路と

を有する信号処理回路。

【請求項６】　送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインタフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、

送信時には、送信すべきデータを所定の暗号モードで暗号化し、受信時には受信パケットデータに含まれる暗号化情報に基づいて受信した暗号化データを復号してアプリケーション側へ出力する暗号処理回路と、

暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路と

を有する信号処理回路。

【請求項７】　上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する

請求項６記載の信号処理回路。

【請求項８】　送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインタフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、

第１の記憶手段と、

第２の記憶手段と、

少なくとも一つの暗号モード情報が設定される保持手段と、

送信データを暗号化すべきモードを指定する制御手段と、

受信パケットデータから上記時間情報および暗号化データに上記暗号化情報を

付加して上記記憶手段に格納する第１の受信回路と、

上記記憶手段に格納された暗号化情報および暗号化データを出力するとともに、時間情報に基づいて受信データをアプリケーション側へ出力すべき時間を指示する第２の受信回路と、

上記第２の受信回路による暗号化情報から暗号化データが暗号化された暗号モードを検出する暗号モード検出回路と、上記制御手段で指定された暗号モード情報または上記暗号モード検出回路で検出した暗号モード情報を上記保持手段に設定された情報の中から選択する暗号モード選択回路と、送信時には上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力し、受信時には上記暗号モード選択回路で選択された暗号モードで上記受信データを復号して、復号データを上記第２の受信回路により指示された時間にアプリケーション側へ出力する暗号エンジン回路とを有する暗号処理回路と、

受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第１の送信回路と、

上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する第２の送信回路と

を有する信号処理回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタルシリアルインタフェースに用いられる信号処理回路に係

り、特にデータの暗号化回路に関するものである。

【０００２】

【従来の技術】

近年、マルチメディア・データ転送のためのインタフェースとして、高速データ転送、リアルタイム転送を実現するＩＥＥＥ（The Institute of Electrical and Electronic Engineers）１３９４、Ｈｉｇｈ　Ｐｅｒｆｏｒｍａｎｃｅ　Ｓｉｒｉａｌ　Ｂｕｓが規格化された。

【０００３】

このＩＥＥＥ１３９４シリアルインタフェースのデータ転送には、従来のRequest,Acknowledge の要求、受信確認を行うアシンクロナス（Asynchronous）転送と、あるノードから１２５μｓに１回必ずデータが送られるアイソクロナス(Isochronous）転送がある。

【０００４】

このように、２つの転送モードを有するＩＥＥＥ１３９４シリアルインタフェースでのデータは、パケット単位で転送が行われる。

【０００５】

図１０は、アイソクロナス通信における１ソースパケットのバイトサイズを示す図である。図１０（Ａ）はＤＶＢ(Digital Video Broadcast）仕様時、図１０（Ｂ）はＤＳＳ(Digital Satelite System）仕様時のパケットサイズを示している。

【０００６】

ＤＶＢ仕様時のソースパケットサイズは、図１０（Ａ）に示すように、４バイトのソースパケットヘッダ（ＳＰＨ；Source Packet Header）と１８８バイトのトランスポートストリームデータの１９２バイトである。

【０００７】

これに対して、ＤＳＳ仕様時のソースパケットサイズは、図１０（Ｂ）に示すように、４バイトのソースパケットヘッダ（ＳＰＨ）、１０バイトの付加データ、および１３０バイトのデータの１４４バイトである。

付加バイトはソースパケットヘッダとデータとの間に挿入される。なお、ＩＥ

ＥＥ１３９４規格では、取り扱う最小データの単位は１クワドレット(quadlet)（＝４バイト＝３２ビット）であるため、トランスポートストリームデータと付加データの合計が３２ビット単位で構成できる設定であることが必要である。

ただし、デフォルトでは付加バイトなしで設定される。

【０００８】

図１１は、ＩＥＥＥ１３９４規格のアイソクロナス通信でデータを送信させるときの元のデータと、実際に送信されるパケットとの対応関係の一例を示す図である。

【０００９】

図１１に示すように、元のデータであるソースパケットは、４バイトのソースパケットヘッダと、データ長を調整するためのパディングデータを付加された後、所定の数のデータブロックに分割される。

なお、パケットを転送するときのデータの単位が１クワドレット（４バイト）であることから、データブロックや各種ヘッダなどのバイト長は、全て４の倍数に設定される。

【００１０】

図１２は、ソースパケットヘッダのフォーマットを示す図である。

図１２に示すように、ソースパケットヘッダのうち、２５ビットには、たとえば上述したＤＶＢ方式等のディジタル衛星放送等で利用されているＭＰＥＧ(Moving Picture Experts Group)－ＴＳ(Transport Stream)データをアイソクロナス通信で送信するときに、ジッタを抑制するために利用されるタイムスタンプ(Time Stamp)が書き込まれる。

【００１１】

そして、このようなパケットヘッダやＣＩＰ(Common Isochronous Packet)ヘッダ等のデータが、所定の数のデータブロックに付加されることによりパケットが生成される。

【００１２】

図１３はアイソクロナス通信用パケットの基本構成例を示す図である。

図１３に示すように、アイソクロナス通信のパケットは、第１クワドレットが

１３９４ヘッダ(Header)、第２クワドレットがヘッダＣＲＣ(Header-CRC)、第３クワドレットがＣＩＰヘッダ１（CIP-Header1)、第４クワドレットがＣＩＰヘッダ２（CIP-Header2)、第５クワドレットがソースパケットヘッダ（ＳＰＨ）で、第６クワドレット以降がデータ領域である。そして、最後のクワドレットがデータＣＲＣ(Data-CRC)である。

【００１３】

１３９４ヘッダは、データ長を表すdata-length 、このパケット転送されるチャネルの番号（０～６３のいずれか）を示すchannel 、処理のコードを表すtcode 、および各アプリケーションで規定される同期コードｓｙにより構成されている。

ヘッダＣＲＣは、パケットヘッダの誤り検出符号である。

【００１４】

ＣＩＰヘッダ１は、送信ノード番号のためのＳＩＤ(Source node ID)領域、データブロックの長さのためのＤＢＳ(Data Block Size) 領域、パケット化におけるデータの分割数のためのＦＮ(Fraction Number) 領域、パディングデータのクワドレット数のためのＱＰＣ(Quadlet Padding Count) 領域、ソースパケットヘッダの有無を表すフラグのためのＳＰＨ領域、アイソクロナスパケットの数を検出するカウンタのためのＤＢＣ (Data Block Continuty Counter) 領域により構成されている。

なお、ＤＢＳ領域は、１アイソクロナスパケットで転送するクワドレット数を表す。

【００１５】

ＣＩＰヘッダ２は、転送されるデータの種類を表す信号フォーマットのためのＦＭＴ領域、および信号フォーマットに対応して利用されるＦＤＦ(Format Dependent Field)領域により構成されている。

【００１６】

ＳＰＨヘッダは、トランスポートストリームパケットが到着した時間に固定の遅延値を加えた値が設定されるタイムスタンプ領域を有している。

また、データＣＲＣは、データフィールドの誤り検出符号である。

【００１７】

上述した構成を有するパケットの送受信を行うＩＥＥＥ１３９４シリアルインタフェースの信号処理回路は、図１４に示すように、主としてＩＥＥＥ１３９４シリアルバスを直接ドライブするフィジカル・レイヤ回路１と、フィジカル・レイヤ回路１のデータ転送をコントロールするリンク・レイヤ回路２とにより構成される。

【００１８】

上述したＩＥＥＥ１３９４シリアルインタフェースにおけるアイソクロナス通信系では、たとえば図１４に示すように、リンク・レイヤ回路２はフィジカル・レイヤ回路１を介してシリアルインタフェースバスＢＳに接続されている。

そして、リンク・レイヤ回路２には、ＭＰＥＧトランスポータやＤＶＣＲ(Digital Video Cassette Recorder) 等のアプリケーション側回路３が接続される。

【００１９】

【発明が解決しようとする課題】

ところで、現在、映画やテレビ放送などの映像データは、著作権との関係等から不正コピーを防止するため、家庭等では、自由にディジタル記録できない。したがって、たとえばディジタル衛星放送用のセット・トップ・ボックスにはディジタルの出力端子が設けられていない。

【００２０】

しがしながら、ＩＥＥＥ１３９４シリアルインタフェースは、映像や音楽などのディジタルデータを異なる機器間で送受信するインタフェースであり、また、近年、家庭用のディジタル録画機器の開発が盛ん行われ、実用に供されてくるようになってきた現状では、家庭等でディジタル記録を行う機会が増えてくることは避けられないことである。

したがって、このような状況に鑑みて不正コピーを有効に防止する機能が必要であるが、ＩＥＥＥ１３９４シリアルインタフェースの信号処理回路では、その機能を備えた構成は未だ実現されていない。

【００２１】

また、この暗号化機能を実現した場合には、連続して複数のパケットデータを

送信する場合に、一つの転送サイクル内で、異なる暗号モードで暗号化されたデータが混在していると、受信側で暗号モードを判別できず、復号できないという不都合が生じないように構成する必要がある。

【００２２】

本発明は、かかる事情に鑑みてなされたものであり、その目的は、異なる機器間で送信または受信するディジタルデータの不正なコピーを防止できる、かつ複数の暗号モードを判別できず、復号できなくなることを防止でき、受信側において受信データを正しく復号することができる信号処理回路を提供することにある。

【００２３】

【課題を解決するための手段】

上記目的を達成するため、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、送信すべきデータを所定の暗号モードで暗号化し、暗号化情報とともに出力する暗号処理回路と、暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路とを有する。

【００２４】

また、本発明では、上記送信回路は、上記暗号化情報をパケットのヘッダの所定の領域に設定する。

【００２５】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、少なくとも一つの暗号モード情報が設定される保持手段と、送信データを暗号化すべきモードを指定する制御手段と、上記制御手段で指定された暗号モード

情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力する暗号エンジン回路とを有する暗号処理回路と、暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路とを有する。

【００２６】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出する信号処理回路であって、記憶手段と、少なくとも一つの暗号モード情報が設定される保持手段と、送信データを暗号化すべきモードを指定する制御手段と、上記制御手段で指定された暗号モード情報を選択する暗号モード選択回路と、上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力する暗号エンジン回路とを有する暗号処理回路と、受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第１の送信回路と、上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインタフェースバスに送信し、かつ、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する第２の送信回路とを有する。

【００２７】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインタフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、送信時には、送信すべきデータを所定の暗号モードで暗号化し、受信時には受信パケットデータに含まれる暗号化情報に基づいて受信した暗号化データを復号してアプリケーション側へ出力する暗号処理回路と、暗号処理回路で暗号化されたデータに、その暗号化情報を付加して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する送信回路とを有する。

【００２８】

また、本発明は、送信すべきデータをパケットデータとしてあらかじめ決められた時間サイクルでシリアルインタフェースバスに送出し、あらかじめ決められた時間サイクルでシリアルインタフェースバスを送信される、データが暗号化され、少なくともその暗号化情報を含むパケットデータを受信してアプリケーション側に出力する信号処理回路であって、第１の記憶手段と、第２の記憶手段と、少なくとも一つの暗号モード情報が設定される保持手段と、送信データを暗号化すべきモードを指定する制御手段と、受信パケットデータから上記時間情報および暗号化データに上記暗号化情報を付加して上記記憶手段に格納する第１の受信回路と、上記記憶手段に格納された暗号化情報および暗号化データを出力するとともに、時間情報に基づいて受信データをアプリケーション側へ出力すべき時間を指示する第２の受信回路と、上記第２の受信回路による暗号化情報から暗号化データが暗号化された暗号モードを検出する暗号モード検出回路と、上記制御手段で指定された暗号モード情報または上記暗号モード検出回路で検出した暗号モ

ード情報を上記保持手段に設定された情報の中から選択する暗号モード選択回路と、送信時には上記暗号モード選択回路で選択された暗号モードで上記送信すべきデータを暗号化して、暗号化データをその暗号化情報とともに出力し、受信時には上記暗号モード選択回路で選択された暗号モードで上記受信データを復号して、復号データを上記第２の受信回路により指示された時間にアプリケーション側へ出力する暗号エンジン回路とを有する暗号処理回路と、受信側で受信データをアプリケーション側へ出力すべき時間情報を生成し、当該時間情報に上記暗号処理回路による暗号化情報を付加して上記暗号化データとともに上記記憶手段に格納する第１の送信回路と、上記記憶手段に格納された時間情報および暗号化情報が付加された暗号化データを読み出し、所定フォーマットのパケットデータを生成するとともに、そのパケットヘッダに上記暗号化情報を設定して上記シリアルインタフェースバスに送信し、複数のパケットの送信時には、上記暗号処理回路による暗号化情報から暗号モードの連続性を確認し、不連続性を確認したときは、上記あらかじめ決められた時間サイクルで送信できる帯域に余裕があったとしても送信を停止させ、異なる暗号モードで暗号化されたデータを次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信する第２の送信回路とを有する。

【００２９】

本発明によれば、送信すべきデータは、暗号化処理回路において指定された暗号モードで暗号化される。

そして、暗号化されたデータは、その暗号化の情報とともに、たとえば記憶手段に一旦格納される。

そして、送信回路により記憶手段から読み出され、たとえば格納された暗号化情報が所定フォーマットのパケットのヘッダに設定されて、暗号化データとともに、あらかじめ決められた時間サイクルでシリアルインタフェースバスに送出される。

また、データ送信において、複数のパケットの送信時には、送信回路で、暗号処理回路による暗号化情報から暗号モードの連続性が確認される。

その結果、不連続性が確認されたときは、あらかじめ決められた時間サイクル

で送信できる帯域に余裕があったとしても送信が停止され、異なる暗号モードで暗号化されたデータは、次のサイクルでパケットデータとして上記シリアルインタフェースバスに送信される。

【００３０】

また、本発明によれば、シリアルインタフェースバスを転送されたパケットデータは受信回路に入力される。

受信回路では、受信パケットデータから暗号化情報および暗号化データが抽出され、たとえば記憶手段に格納される。

記憶手段に格納された暗号化情報および暗号化データは、暗号処理回路に読み出される。

そして、暗号処理回路においては、読み出した暗号化情報に基づいて受信暗号化データが復号されてアプリケーション側へ出力される。

【００３１】

【発明の実施の形態】

図１は、ＩＥＥＥ１３９４シリアルインタフェースに適用される本発明に係る信号処理回路の一実施形態を示すブロック構成図である。

【００３２】

この信号処理回路は、リンク・レイヤ回路１０、フィジカル・レイヤ回路２０、ホストコンピュータとしてのＣＰＵ３０により構成されている。また、リンクレイヤ回路１０には、アプリケーション側回路４０が接続されている。

アプリケーション側回路４０は、図１に示すように、ＭＰＥＧトランスポータ４１、Ｄ／Ａ(Digital/Analog)コンバータ４２、ＩＥＣ９５８ディジタルオーディオ回路４３により構成される。また、４４はクロック供給回路としてのＰＬＬ回路を示している。

なお、以下では、アプリケーション側回路４をＭＰＥＧトランスポータ４１として説明する。

【００３３】

リンク・レイヤ回路１０は、ＣＰＵ３０の制御の下、アシンクロナス転送およびアイソクロナス転送の制御、並びにフィジカル・レイヤ回路２０の制御を行う

。

具体的には、図１に示すように、リンクコア(Link Core))１０１、ホストインタフェース回路（HOST I/F）１０２、アプリケーションインタフェース回路（AP I/F）１０３、アシンクロナス通信の送信用ＦＩＦＯ（AT-FIFO)１０４、アシンクロナス通信の受信用ＦＩＦＯ（AR-FIFO)１０５、インサートパケットバッファ（ＩＰＢ）１０６、暗号処理回路（ＣＰＨ）１０７、第１の送信回路としてのアイソクロナス通信用送信前処理回路(TXOPRE)１０８、第２の送信回路としてのアイソクロナス通信用送信後処理回路(TXOPRO)１０９、第１の受信回路としてのアイソクロナス通信用受信前処理回路(TXIPRE)１１０、第２の受信回路としてのアイソクロナス通信用受信後処理回路(TXIPRO)１１１、アイソクロナス通信の送信用ＦＩＦＯ(IT-FIFO) １１２、アイソクロナス通信の受信用ＦＩＦＯ(IR-FIFO)１１３および保持手段としてのコンフィギュレーションレジスタ（Configuration Register、以下ＣＦＲという）１１４により構成されている。

【００３４】

図１の回路おいて、ホストインタフェース回路１０２、送信用ＦＩＦＯ１０４、受信用ＦＩＦＯ１０５およびリンクコア１０１によりアシンクロナス通信系回路が構成される。

そして、アプリケーションインタフェース回路１０３、暗号処理回路１０７、送信前処理回路１０８、送信後処理回路１０９、受信前処理回路１１０、受信後処理回路１１１、送信用ＦＩＦＯ１１２、受信用ＦＩＦＯ１１３およびリンクコア１０１によりアイソクロナス通信系回路が構成される。

【００３５】

リンクコア１０１は、アシンクロナス通信用パケットおよびアイソクロナス通信用パケットの送信回路、受信回路、これらパケットのＩＥＥＥ１３９４シリアルバスＢＳを直接ドライブするフィジカル・レイヤ回路２０とのインタフェース回路、１２５μｓ毎にリセットされるサイクルタイマ、サイクルモニタやＣＲＣ回路から構成されている。そして、たとえばサイクルタイマ等の時間データ等はＣＦＲ１１１を通してアイソクロナス通信系処理回路に供給される。

【００３６】

ホストインタフェース回路１０２は、主としてホストコンピュータとしてのＣＰＵ３０と送信用ＦＩＦＯ１０４、受信用ＦＩＦＯ１０５とのアシンクロナス通信用パケットの書き込み、読み出し等の調停、並びに、ＣＰＵ３０とＣＦＲ１１４との各種データの送受信の調停を行う。

たとえばＣＰＵ３０からは、アイソクロナスパケットを暗号化する、後述する複数のモード（キー；ｋｅｙ）が設定され、設定された暗号モードのうちの一つを選択して暗号処理回路１０７が暗号化すべき暗号キー選択情報が、ホストインタフェース１０２を通してＣＦＲ１１４にセットされる。

また、たとえばＣＰＵ３０からは、アイソクロナス通信用パケットのＳＰＨ（ソースパケットヘッダ）に設定されるタイムスタンプ用遅延時間Txdelay がホストインタフェース１０２を通してＣＦＲ１１４にセットされる。

さらに、ＣＰＵ３０からは、たとえば通常のＭＰＥＧのトランスポートストリームデータの間に制御用パケットであるインサートパケットデータを挿入する必要が生じたとき、ＣＦＲ１１４のレジスタＩＰＴｘＧｏに論理「１」がセットされる。

【００３７】

アプリケーションインタフェース回路１０３は、アプリケーション側回路４０、たとえばＭＰＥＧトランスポータ４１と暗号処理回路１０７と制御信号等を含む、暗号化前および復号化後のデータの送受信の調停を行う。

【００３８】

送信用ＦＩＦＯ１０４には、ＩＥＥＥ１３９４シリアルバスＢＳに伝送させるアシンクロナス通信用パケットが格納され、受信用ＦＩＦＯ１０５にはＩＥＥＥ１３９４シリアルインタフェースバスＢＳを伝送されてきたアシンクロナス通信用パケットが格納される。

【００３９】

インサートパケットバッファ１０６には、たとえば所望のパケットデータがＣＰＵ３０から書き込まれる。

インサートパケットバッファ１０６の容量は、たとえば１８８バイトであり、

１８８バイトまでのデータが有効で、この容量を超えたデータに関しては送信されない。

送信するデータが１８８バイト以下の場合は、書き込まれたデータ以外が「１」にセットされて送信される。

インサートパケットバッファ１０６に一度書き込まれたデータは、再び書き込みが行われるまで、その値を保持される。

インサートパケットバッファ１０６に書き込まれたデータは、暗号処理回路１０７で暗号化されて送信前処理回路１０８を介して送信用ＦＩＦＯ１１２に転送されるが、転送時には、上述したＣＦＲ１１４のレジスタＩＰＴｘＧｏが「１」に設定され、転送が終了した場合には自動的に「０」に設定され、ＣＰＵ３０はこれを確認することで転送終了を確認する。

【００４０】

暗号処理回路１０７は、データ送信時には、ＣＰＵ３０からＣＦＲ１１４に設定された暗号キー選択情報に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された複数の暗号モード（キー；ｋｅｙ）のうち一の暗号キーを選択し、選択しが暗号キーにより、アプリケーションインタフェース回路１０３を介して入力した送信すべきデータをたとえば所定の共通鍵暗号方式により暗号化し、送信前処理回路１０８に出力する。

また、暗号処理回路１０７は、受信後処理回路１１１を介して入力した暗号化されたデータの暗号化に用いられた暗号モード（キー）を検出し、その暗号キー情報に基づいて暗号化データを復号してアプリケーションインタフェース回路１０３に出力する。

【００４１】

ここで、暗号モードおよび暗号キーの例について図２に関連付けて説明する。

暗号モードには、図２（Ａ）に示すように、モードＡ，モードＢ、およびモードＣの３種類があり、これに加えて暗号化なしがある。

そし、各暗号モードＡ，Ｂ，Ｃの内容は次の通りである。

暗号モードＡはコピーを認めない(Never Cppy)、暗号モードＢは一度だけコピーを認める(Copy Once)、暗号モードＣはこれ以上のコピーを認めないおよび暗

号化しない(No MOre Copy)である。

また、暗号キーには、図２（Ｂ）に示すように、偶数(Even)キー、および奇数(Odd) キーの２種類がある。

したがって、暗号化を行う暗号キーとしては、①モードＡ，奇数、②モードＡ，偶数、③モードＢ，奇数、④モードＢ，偶数、⑤モードＣ，奇数、⑥モードＣ，偶数の６種類がある。

【００４２】

図３は、暗号処理回路１０７の構成例を示すブロック図である。

暗号処理回路１０７は、図３に示すように、暗号モード選択回路１０７１、暗号モード検出回路１０７２、マルチプレクサ１０７３、および暗号エンジン回路１０７４により構成されている。

【００４３】

暗号モード選択回路１０７１は、データ送信時には、ＣＰＵ３０からＣＦＲ１１４に設定された暗号キー選択信号（情報）Ｓ１１４に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された６個の暗号モード（キー；ｋｅｙ）のうちの一の暗号キーを選択し、暗号エンジン回路１０７４に出力する。

また、データ受信時には、暗号モード検出回路１０７２からの暗号キー選択信号Ｓ１０７２に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された６個の暗号モード（キー；ｋｅｙ）のうち、一の暗号キーを選択し、暗号エンジン回路１０７４に出力する。

【００４４】

暗号モード検出回路１０７２は、受信後処理回路１１１を介して入力し暗号化情報から、データの暗号化に用いられた暗号モード（キー）を検出し、検出結果を暗号キー選択信号Ｓ１０７２として暗号モード選択回路１０７１に出力する。

【００４５】

マルチプレクサ１０７３は、送信時にはアプリケーションインタフェース回路１０３を介した送信データを暗号エンジン回路１０７４に入力させ、受信時には受信後処理回路１１１による暗号化されている受信データを暗号エンジン回路１０７４に入力させる。

【００４６】

暗号エンジン回路１０７４は、送信時には、マルチプレクサ１０７３を介して入力した送信データを、暗号モード選択回路１０７１により指定された暗号キーに基づいて暗号化してその暗号化情報とともに送信前処理回路１０８に出力し、受信時には、マルチプレクサ１０７３を介して入力した受信データを、暗号モード選択回路１０７１により指定された暗号キーに基づいて暗号化データを復号してアプリケーションインタフェース回路１０３に出力する。

【００４７】

送信前処理回路１０８は、暗号処理回路１０７による送信しべき暗号化データを受けて、ＩＥＥＥ１３９４規格のアイソクロナス通信用としてクワドレット（４バイト）単位にデータ長を調整し、かつ４バイト（＋４ビット）のソースパケットヘッダ（ＳＰＨ）を付加し、送信用ＦＩＦＯ１１２に格納する。

【００４８】

送信前処理回路１０８は、送信用ＦＩＦＯ１１２に送信データを格納するに際して、図４（Ａ）に示すように、４バイト（０～３１ビット）のソースパケットヘッダに４ビット（３２～３６ビット）を付加し、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報を設定して格納するとともに、図４（Ｂ）に示すように、データ領域の４バイト（０～３１ビット）の最大長を示すデータペイロード(Data Payload)に同じく４ビット（３２～３６ビット）を付加し、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報を設定して格納する。

【００４９】

暗号化情報は、モードがビット〔３５：３４〕の２ビットで示され、キーの種類をビット〔３３〕の１ビットで示され、内容に応じてこれら３ビットが、図２中ｓｙ〔３：２〕およびｓｙ〔１〕のように設定される。ただし、ビット３２は未使用である。

すなわち、モードＡで偶数キーの場合には〔１１１〕、モードＢで偶数キーの場合には〔１０１〕、モードＣで偶数キーの場合には〔０１１〕、モードＡで奇数キーの場合には〔１１０〕、モードＢで奇数キーの場合には〔１００〕、モー

ドＣで奇数キーの場合には〔０１０〕に設定される。

また、暗号化なしの場合には、ビット〔３５：３４〕が〔００〕に設定される。このとき、ビット〔３３〕は意味を持たない。

【００５０】

また、送信前処理回路１０８は、ソースパケットヘッダを付加するときに受信側のデータ出力時間を決定するタイムスタンプを設定するが、この設定は以下のように行われる。

まず、アプリケーション側回路４０、たとえばＭＰＥＧトランスポータ４１からパケットの最終データを受け取ったタイミングで内部のサイクルレジスタの値をラッチする。

次に、ＣＰＵ３０からホストインタフェース１０２を介してＣＦＲ１１４にセットされた遅延時間Txdelay を上記サイクルレジスタの値に加算する。

そして、加算した値をタイムスタンプとして、受け取ったパケットのソースパケットヘッダに挿入（設定）する。

【００５１】

図４（Ａ）は、ソースパケットヘッダにおけるタイムスタンプの具体的な構成を説明するための図である。

図４（Ａ）に示すように、受信側のデータ出力時間を決定するためのタイムスタンプは、２５ビットで現時刻を表す。

すなわち、タイムスタンプは２５ビットで構成され、下位１２ビットがサイクルオフセットＣＯ(cycle-offset)領域、上位１３ビットがサイクルカウントＣＣ(cycle-count) 領域として割り当てられている。

サイクルオフセットは０～３０７１（１２ｂ　１０１１１１１１１１１）の１２５μｓをカウントし（クロックＣＬＫ＝２４．５７６ＭＨｚ）、サイクルカウントは０～７９９９（１３ｂ　１１１１１００１１１１１）の１秒をカウントするものである。

したがって、原則として、タイムスタンプの下位１２ビットは３０７２以上を示すことはなく、上位１３ビットは８０００以上を示すことはない。

【００５２】

送信後処理回路１０９は、送信用ＦＩＦＯ１１２に格納されたソースパケットヘッダを含むデータに対して図５および図１３に示すように、１３９４ヘッダ、ＣＩＰヘッダ１，２を付加してリンクコア１０１の送信回路に出力する。

具体的には、図５に示すように、データ長を表すdata-length 、このパケット転送されるチャネルの番号（０～６３のいずれか）を示すchannel 、処理のコードを表すtcode 、および暗号化情報を示すｓｙにより構成した１３９４ヘッダ、さらに図１３に示すように、送信ノード番号のためのＳＩＤ(Source node ID)領域、データブロックの長さのためのＤＢＳ(Data Block Size) 領域、パケット化におけるデータの分割数のためのＦＮ(Fraction Number) 領域、パディングデータのクワドレット数のためのＱＰＣ(Quadlet Padding Count) 領域、ソースパケットヘッダの有無を表すフラグのためのＳＰＨ領域、アイソクロナスパケットの数を検出するカウンタのためのＤＢＣ領域により構成したＣＩＰヘッダ１、並びに転送されるデータの種類を表す信号フォーマットのためのＦＭＴ領域、および信号フォーマットに対応して利用されるＦＤＦ(Format Dependent Field)領域により構成したＣＩＰヘッダ２を付加する。

【００５３】

なお、１３９４ヘッダに設定される暗号化情報ｓｙは、１３９４ヘッダのビット〔３，２，１〕の３ビットが割り当てられる。その内容は、ＦＩＦＯ１１２に格納されたソースパケットヘッダに付加された暗号化情報に基づいて設定される。

暗号化情報は、モードがビット〔３：２〕の２ビットで示され、キーの種類をビット〔１〕の１ビットで示され、内容に応じてこれら３ビットが、図２中ｓｙ〔３：２〕およびｓｙ〔１〕のように設定される。

すなわち、モードＡで偶数キーの場合には〔１１１〕、モードＢで偶数キーの場合には〔１０１〕、モードＣで偶数キーの場合には〔０１１〕、モードＡで奇数キーの場合には〔１１０〕、モードＢで奇数キーの場合には〔１００〕、モードＣで奇数キーの場合には〔０１０〕に設定される。

また、暗号化なしの場合には、ビット〔３：２〕が〔００〕に設定される。こ

のとき、ビット〔１〕は意味を持たない。

【００５４】

また、送信後処理回路１０９は、図６に示すように、複数のパケットの送信時に、ＦＩＦＯ１１２から送信データを読み出した際に暗号モードの連続性を確認し、不連続性を確認したときは、その１３９４規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア１０１の送信回路に指示する暗号モード連続性判定回路１０９１を有している。

【００５５】

暗号モード連続性判定回路１０９１を設けた理由を以下に説明する。

図７に示すように、１３９４規格の１サイクルのうちに、１パケットのみを送信する場合には、暗号モードがたとえばモードＡ／偶数とモード／奇数と切り換わっても、各送信パケットには１３９４ヘッダのｓｙ領域に暗号化情報が付加されることから、受信側で暗号モードを判別でき、復号可能である。

【００５６】

これに対して、複数のパケットを暗号化して送信する場合には、暗号モード連続性判定回路１０９１を設けない場合には、図８に示すように、その切り替えタイミングにより１３９４規格の１サイクルのうちに、異なる暗号キーで暗号化されたデータが混在してしまう。

この場合、混在したデータに一つの１３９４ヘッダが付加されるのみであることから、受信側で複数の暗号モードを判別できず、復号することができなくなる。

【００５７】

そこで、暗号モード連続性判定回路１０９１を設けて、複数をパケットの送信時に、ＦＩＦＯ１１２から送信データを読み出した際に暗号モードの連続性を確認し、不連続性を確認したときは、その１３９４規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されてパケットを送信するように、リンクコア１０１の送信回路に指示して、図９に示すように、１３９４規格の１サイクル内では、一つの暗号モード

で暗号化されたデータのみを送信し、異なる暗号モードで暗号化されたデータは次のサイクルで送信するように構成している。

【００５８】

受信前処理回路１１０は、リンクコア１０１を介してＩＥＥＥ１３９４シリアルバスＢＳを伝送されてきたアイソクロナス通信用パケットを受けて、受信パケットの１３９４ヘッダ、ＣＩＰヘッダ１，２等の内容を解析し、４バイト（＋４ビット）のソースパケットヘッダ（ＳＰＨ）を付加し、受信用ＦＩＦＯ１１３に格納する。

【００５９】

受信前処理回路１１０は、受信用ＦＩＦＯ１１３に受信データを格納するに際して、受信パケットの１３９４ヘッダのｓｙ領域のビット３，２，１に設定されている暗号化情報を、送信前処理１０８と同様に格納するソースパケットヘッダおよびデータに付加する。

すなわち、図４（Ａ）に示すように、４バイト（０～３１ビット）のソースパケットヘッダに４ビット（３２～３６ビット）を付加し、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報を設定して格納するとともに、図４（Ｂ）に示すように、データ領域の４バイト（０～３１ビット）の最大長を示すデータペイロード(Data Payload)に同じく４ビット（３２～３６ビット）を付加し、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報を設定して格納する。

【００６０】

暗号化情報は、モードがビット〔３５：３４〕の２ビットで示され、キーの種類をビット〔３３〕の１ビットで示され、内容に応じてこれら３ビットが、図２中ｓｙ〔３：２〕およびｓｙ〔１〕のように設定される。ただし、ビット３２は未使用である。

すなわち、モードＡで偶数キーの場合には〔１１１〕、モードＢで偶数キーの場合には〔１０１〕、モードＣで偶数キーの場合には〔０１１〕、モードＡで奇数キーの場合には〔１１０〕、モードＢで奇数キーの場合には〔１００〕、モードＣで奇数キーの場合には〔０１０〕に設定される。

また、暗号化なしの場合には、ビット〔３５：３４〕が〔００〕に設定される。このとき、ビット〔３３〕は意味を持たない。

【００６１】

受信後処理回路１１１は、受信用ＦＩＦＯ１１３に格納されたソースパケットヘッダおよびデータを読み出して、付加された暗号化情報を暗号処理回路１０７の暗号モード検出回路１０７２に出力し、暗号化データをマルチプレクサ１７３を介して暗号エンジン回路１０７４に入力させる。

また、受信後処理回路１１１は、データ読み出し時においては、ＦＩＦＯ１１３に格納されたソースパケットヘッダのタイムスタンプの時間データを読み出し、読み出したタイムスタンプデータ（ＴＳ）とリンクコア１０１内にあるサイクルタイマによるサイクルタイム（ＣＴ）を比較し、サイクルタイムＣＴがタイムスタンプデータＴＳより大きい場合に、暗号エンジン回路１０７４で復号化されたデータをアプリケーションインタフェース回路１０３を介し、たとえばＭＰＥＧ用トランスポートストリームデータとしてＭＰＥＧトランスポータ４１へ出力させる。

【００６２】

次に、ＩＥＥＥ１３９４シリアルインタフェースバスＢＳを伝送されるアイソクロナス通信用パケットの送信動作および受信動作を説明する。

【００６３】

まず、ＣＰＵ３０からＣＦＲ１１４に、アイソクロナスパケットを暗号化する複数のモード（キー；ｋｅｙ）が設定される。

そして、ＩＥＥＥ１３９４シリアルインタフェースバスＢＳにアイソクロナス通信用パケットを送出する場合には、設定された暗号モードのうちの一つを選択して暗号処理回路１０７が暗号化すべき暗号キー選択情報が、ＣＰＵ３０からホストインタフェース１０２を通してＣＦＲ１１４にセットされる。また、ＣＰＵ３０からは、アイソクロナス通信用パケットのＳＰＨ（ソースパケットヘッダ）に設定されるタイムスタンプ用遅延時間Txdelay がホストインタフェース１０２を通してＣＦＲ１１４にセットされる。

【００６４】

これと並行して、アプリケーション側回路４０のたとえばＭＰＥＧトランスポータ４１によるＭＰＥＧトランスポートストリームデータが、アプリケーションインタフェース回路１０３を介して暗号処理回路１０７に入力される。

【００６５】

暗号処理回路１０７では、送信時にはアプリケーションインタフェース回路１０３を介した送信データが、マルチプレクサ１０７３を介して暗号エンジン回路１０７４に入力される。

また、暗号モード選択回路１０７１において、ＣＰＵ３０からＣＦＲ１１４に設定された暗号キー選択信号（情報）Ｓ１１４に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された６個の暗号モード（キー；ｋｅｙ）のうちの一の暗号キーが選択され、その情報が暗号エンジン回路１０７４に供給される。

【００６６】

暗号エンジン回路１０７４においては、マルチプレクサ１０７３を介して入力した送信データが、暗号モード選択回路１０７１により指定された暗号キーに基づいて暗号化されて送信前処理回路１０８に出力される。

【００６７】

送信前処理回路１０８では、暗号処理回路１０７による送信しべき暗号化データを受けて、ＩＥＥＥ１３９４規格のアイソクロナス通信用としてクワドレット（４バイト）単位にデータ長が調整され、かつ４バイト（＋４ビット）のソースパケットヘッダ（ＳＰＨ）を付加されて送信用ＦＩＦＯ１１２に格納される。

このとき、送信前処理回路１０８では、送信用ＦＩＦＯ１１２に送信データを格納するに際して、４バイト（０～３１ビット）のソースパケットヘッダに４ビット（３２～３６ビット）が付加され、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報が設定され、併せて、データ領域の４バイト（０～３１ビット）の最大長を示すデータペイロード(Data Payload)に同じく４ビット（３２～３６ビット）が付加され、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報が設定されて格納される。

【００６８】

ＦＩＦＯ１１２に格納された送信データは、送信後処理回路１０９により読み出され、ソースパケットヘッダを含むデータに対して１３９４ヘッダ、ＣＩＰヘッダ１，２が付加されてリンクコア１０１の送信回路に出力される。

このとき、付加ビットに設定されていた暗号化情報ｓｙは、１３９４ヘッダのビット〔３，２，１〕の３ビットに割り当てられてる。なお、その内容は、ＦＩＦＯ１１２に格納されたソースパケットヘッダに付加された暗号化情報に基づいて設定される。

【００６９】

そして、リンクコア１０１の送信回路に入力されたパケットデータは、フィジカル・レイヤ回路２０を介してＩＥＥＥ１３９４シリアルインタフェースバスＢＳにアイソクロナス通信用パケットとして送出される。

【００７０】

また、複数のパケットが暗号化されて送信される場合には、送信後処理回路１０９における暗号モード連続性判定回路１０９１において、ＦＩＦＯ１１２から送信データを読み出した際に暗号モードの連続性が確認される。

そして、不連続性が確認されたときは、その１３９４規格の送信サイクルで送信できる帯域に余裕があったとしても送信が停止され、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア１０１の送信回路に指示される。

これにより、１３９４規格の１サイクル内では、一つの暗号モードで暗号化されたデータのみが送信され、異なる暗号モードで暗号化されたデータは次のサイクルで送信される。

したがって、受信側で的確に暗号が解読され、データが復号される。

【００７１】

ＩＥＥＥ１３９４シリアルバスＢＳを伝送されてきた、１３９４ヘッダに暗号化情報が設定されてるアイソクロナス通信用パケットは、フィジカル・レイヤ回路１０、リンクコア１０１を介して受信前処理回路１１０に入力される。

【００７２】

受信前処理回路１１０では、受信パケットの１３９４ヘッダ、ＣＩＰヘッダ１，２等の内容が解析され、ソースパケットヘッダとデータがＦＩＦＯ１１３に書き込まれる。

このとき、受信前処理回路１１０においては、受信用ＦＩＦＯ１１３に受信データを格納するに際して、４バイト（０～３１ビット）のソースパケットヘッダに４ビット（３２～３６ビット）が付加され、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報が設定され、併せて、データ領域の４バイト（０～３１ビット）の最大長を示すデータペイロード(Data Payload)に同じく４ビット（３２～３６ビット）が付加され、この付加ビットのうちの３３ビット、３４ビット、および３５ビットの３ビットを用いて暗号化情報が設定されて格納される。

【００７３】

そして、ＦＩＦＯ１１３に格納されたソースパケットヘッダおよび受信データは、受信後処理回路１１１により読み出され、付加ビットの暗号化情報が暗号処理回路１０７の暗号モード検出回路１０７２に供給され、暗号化データをマルチプレクサ１７３を介して暗号エンジン回路１０７４に供給される。

また、受信後処理回路１１１では、ＦＩＦＯ１１３に格納されたソースパケットヘッダのタイムスタンプの時間データが読み出され、読み出したタイムスタンプデータ（ＴＳ）とリンクコア１０１内にあるサイクルタイマによるサイクルタイム（ＣＴ）を比較し、サイクルタイムＣＴがタイムスタンプデータＴＳより大きい場合に、データ出力指示が暗号処理回路１０７の暗号エンジン回路１０７４に供給される。

【００７４】

暗号処理回路１０７では、暗号モード検出回路１０７２において、受信後処理回路１１１を介して入力した暗号化されたデータに付加されている暗号化情報から、データの暗号化に用いられた暗号モード（キー）が検出される。そして、その検出結果が暗号キー選択信号Ｓ１０７２として暗号モード選択回路１０７１に出力される。

暗号モード選択回路１０７１においては、暗号キー選択信号Ｓ１０７２に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された６個の暗号モード（キー；ｋｅｙ）のうちの一の暗号キーが選択され、その情報が暗号エンジン回路１０７４に供給される。

【００７５】

暗号エンジン回路１０７４は、マルチプレクサ１０７３を介して入力した受信データが、暗号モード選択回路１０７１により指定された暗号キーに基づいて復号される。

そして、復号されたデータが受信後処理回路１１１による指示時間に、アプリケーションインタフェース回路１０３を介し、たとえばＭＰＥＧ用トランスポートストリームデータとしてＭＰＥＧトランスポータ４１へ出力される。

【００７６】

以上説明したように、本実施形態によれば、データ送信時には、ＣＰＵ３０からＣＦＲ１１４に設定された暗号キー選択信号Ｓ１１４に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された６個の暗号モードのうちの一の暗号キーを選択し、データ受信時には、暗号モード検出回路１０７２からの暗号キー選択信号Ｓ１０７２に基づき、ＣＰＵ３０からＣＦＲ１１４に設定された６個の暗号モードのうち、一の暗号キーを選択する暗号モード選択回路１０７１と、受信パケットに付加されていた暗号化情報から、データの暗号化に用いられた暗号モードを検出し、検出結果を暗号キー選択信号Ｓ１０７２として暗号モード選択回路１０７１に出力する暗号モード検出回路１０７２と、送信時には、マルチプレクサ１０７３を介して入力した送信データを、暗号モード選択回路１０７１により指定された暗号キーに基づいて暗号化し、受信時には、マルチプレクサ１０７３を介して入力した受信データを、暗号モード選択回路１０７１により指定された暗号キーに基づいて暗号化データを復号する暗号エンジン回路１０７４とを有する暗号処理回路１０７と、送信時に、１３９４ヘッダに暗号化情報を設定して所定の送信パケットとして出力する送信後処理回路１０９とを設けたので、異なる機器間で送信または受信するディジタルデータの不正なコピーを防止でき、しかも良好なアイソクロナス通信を実現できる利点がある。

【００７７】

また、本実施形態では、暗号モード連続性判定回路１０９１を設けて、複数をパケットの送信時に、ＦＩＦＯ１１２から送信データを読み出した際に暗号モードの連続性を確認し、不連続性を確認したときは、その１３９４規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア１０１の送信回路に指示して、１３９４規格の１サイクル内では、一つの暗号モードで暗号化されたデータのみを送信し、異なる暗号モードで暗号化されたデータは次のサイクルで送信するように構成したので、受信側で複数の暗号モードを判別できず、復号することができなくなるということを防止でき、受信側において暗号モードに応じて正しく復号することができる。

【００７８】

なお、本実施形態では、アプリケーション側データとしてＭＰＥＧトランスポートストリームデータを例に説明したが、本発明はこれに限定されず、ディジタルオーディオ等、各ディジタルデータに適用できることはいうまでもない。

【００７９】

【発明の効果】

以上説明したように、本発明によれば、異なる機器間で送信または受信するディジタルデータの不正なコピーを防止できることはもとより、複数の暗号モードを判別できず、復号できなくなることを防止でき、受信側において受信データを正しく復号することができる信号処理回路を実現できる利点がある。

【図面の簡単な説明】

【図１】

ＩＥＥＥ１３９４シリアルインタフェースに適用される本発明に係るＭＰＥＧ用信号処理回路の一実施形態を示すブロック構成図である。

【図２】

本発明に係る暗号モードおよび暗号キーの例について説明するための図である。

【図３】

本発明に係る暗号処理回路の構成例を示すブロック図である。

【図４】

ＦＩＦＯに暗号化データを格納する場合に付加する暗号化情報の一形態を示す図である。

【図５】

送信時に１３９４ヘッダに暗号化情報を設定する一例を説明するための図である。

【図６】

本発明に係る送信後処理回路に暗号モード連続性判定回路を設けた例を示す図である。

【図７】

１サイクルに１パケットを送信する場合の通信形態を示す図である。

【図８】

１サイクルに複数のデータを送信する場合であって、暗号モード連続性判定回路を設けていない場合の通信形態を示す図である。

【図９】

１サイクルに複数のデータを送信する場合であって、暗号モード連続性判定回路を設けた場合の通信形態を示す図である。

【図１０】

アイソクロナス通信における１ソースパケットのバイトサイズを示す図であって、（Ａ）はＤＶＢ仕様時、（Ｂ）はＤＳＳ仕様時のパケットサイズを示す図である。

【図１１】

ＩＥＥＥ１３９４規格のアイソクロナス通信でデータを送信させるときの元のデータと、実際に送信されるパケットとの対応関係の一例を示す図である。

【図１２】

ソースパケットヘッダのフォーマットを示す図である。

【図１３】

アイソクロナス通信用パケットの基本構成例を示す図である。

【図１４】

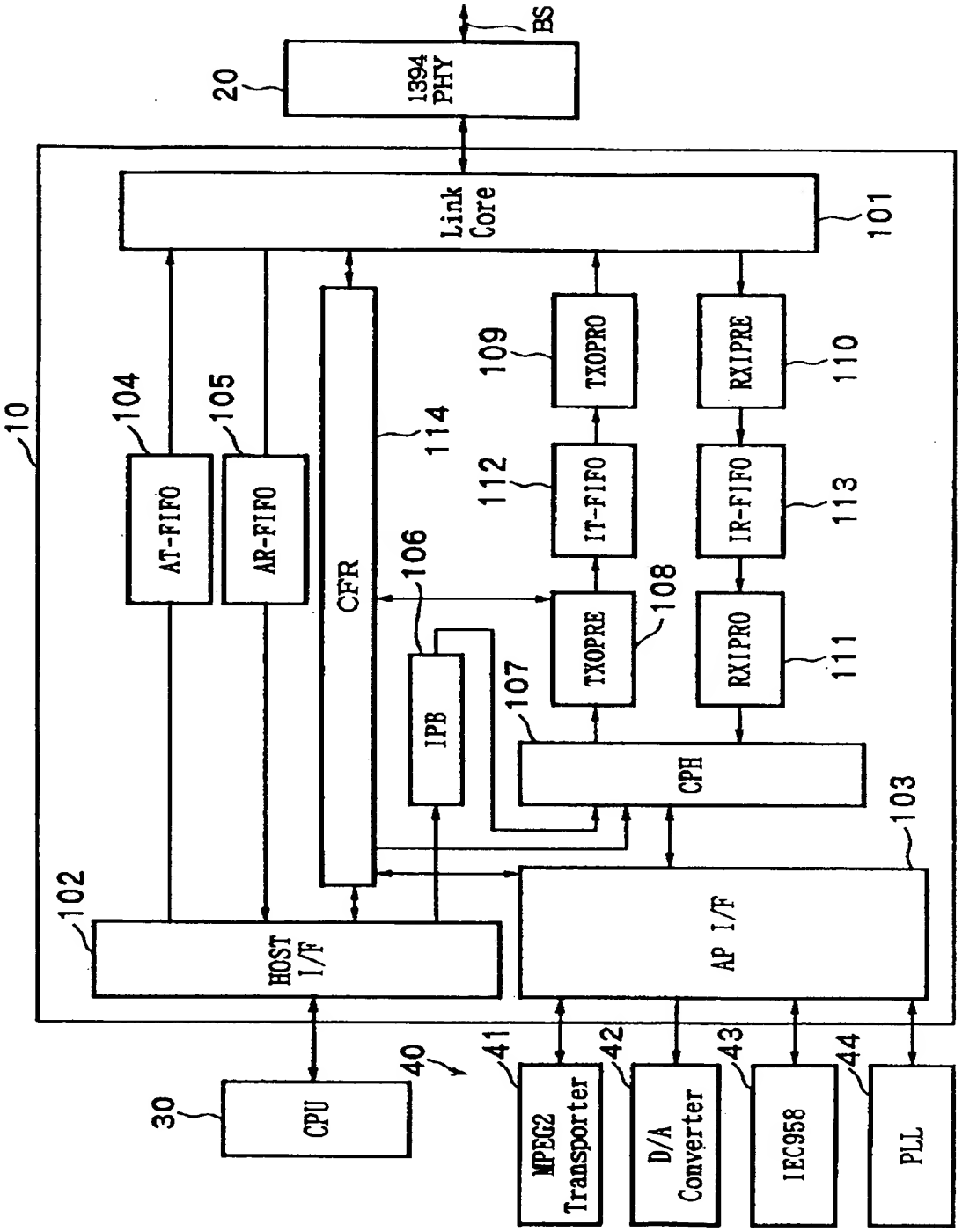
ＩＥＥＥ１３９４シリアルインタフェースにおけるアイソクロナス通信系回路の基本構成を示すブロック図である。

【符号の説明】

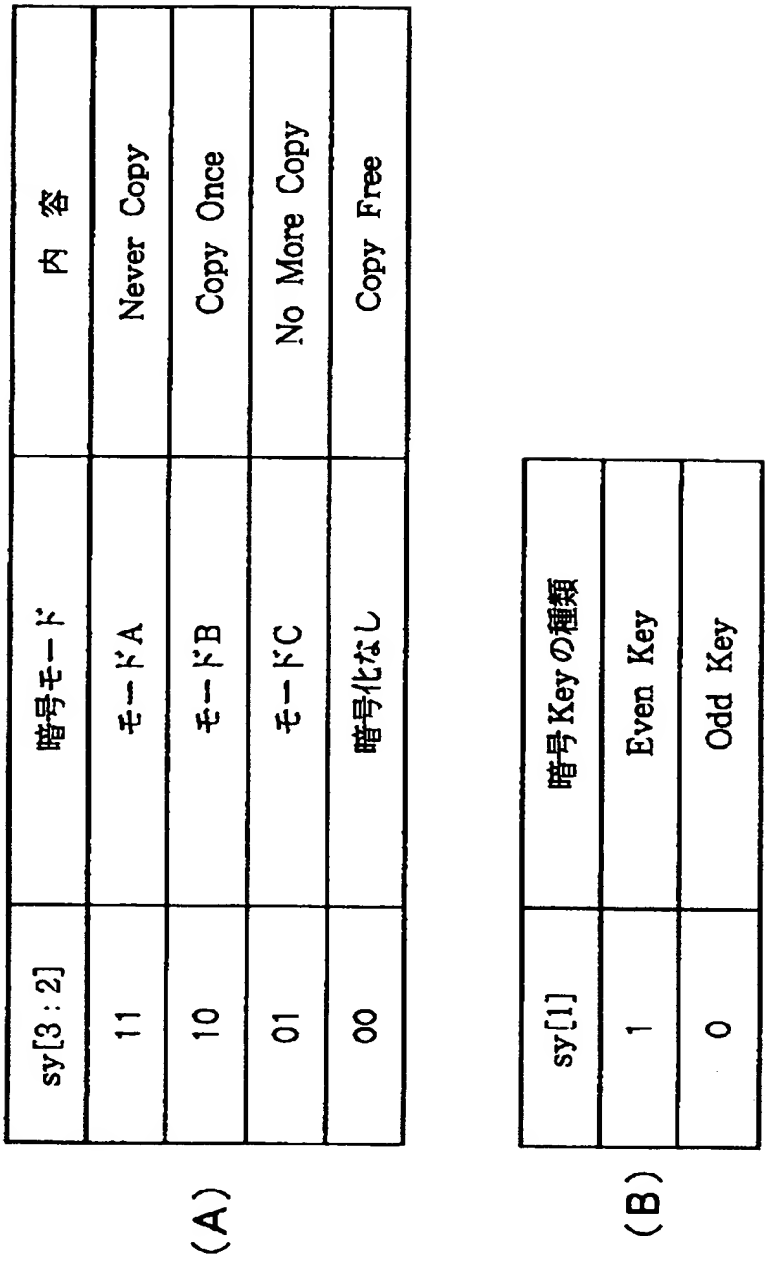
１０…リンク・レイヤ回路、１０１…リンクコア(Link Core))、１０２…ホストインタフェース回路（Host I/F）、１０３…アプリケーションインタフェース回路（AP I/F）、１０４…アシンクロナス通信の送信用ＦＩＦＯ（AT-FIFO)、１０５…アシンクロナス通信の受信用ＦＩＦＯ(AR-FIFO)、１０６…インサートパケットバッファ（ＩＰＢ）、１０７…暗号処理回路、１０７１…暗号モード選択回路、１０７２…暗号モード検出回路、１０７３…マルチプレクサ、１０７４…暗号エンジン回路、１０８…アイソクロナス通信用送信前処理回路(TXOPRE)、１０９…アイソクロナス通信用送信後処理回路(TXOPRO)、１０９１…暗号モード連続性判定回路、１１０…アイソクロナス通信用受信前処理回路(TXPRE)、１１１…アイソクロナス通信用受信後処理回路(TXIPRO、１１２…アイソクロナス通信の送信用ＦＩＦＯ(IT-FIFO)、１１３…アイソクロナス通信の受信用ＦＩＦＯ(IR-FIFO)、１１４…コンフィギュレーションレジスタ（ＣＦＲ）、２０…フィジカル・レイヤ回路、３０…ＣＰＵ、４０…アプリケーション側回路、４１…ＭＰＥＧトランスポータ、４２…Ｄ／Ａコンバータ、４３…ＩＥＣ９５８ディジタルオーディオ回路、４４…ＰＬＬ回路。

【書類名】　図面

【図１】


BS
20
1394 PHY
Link Core
101
10
104
105
114
109
TXOPRO
RX1PRE
110
AT-FIFO
AR-FIFO
CFR
112
IT-FIFO
IR-FIFO
113
106
108
TXOPRE
RX1PRO
111
IPB
107
CPH
103
102
HOST I/F
AP I/F
30
CPU
40
41
MPEG2 Transporter
42
D/A Converter
43
IEC958
44
PLL

【図２】



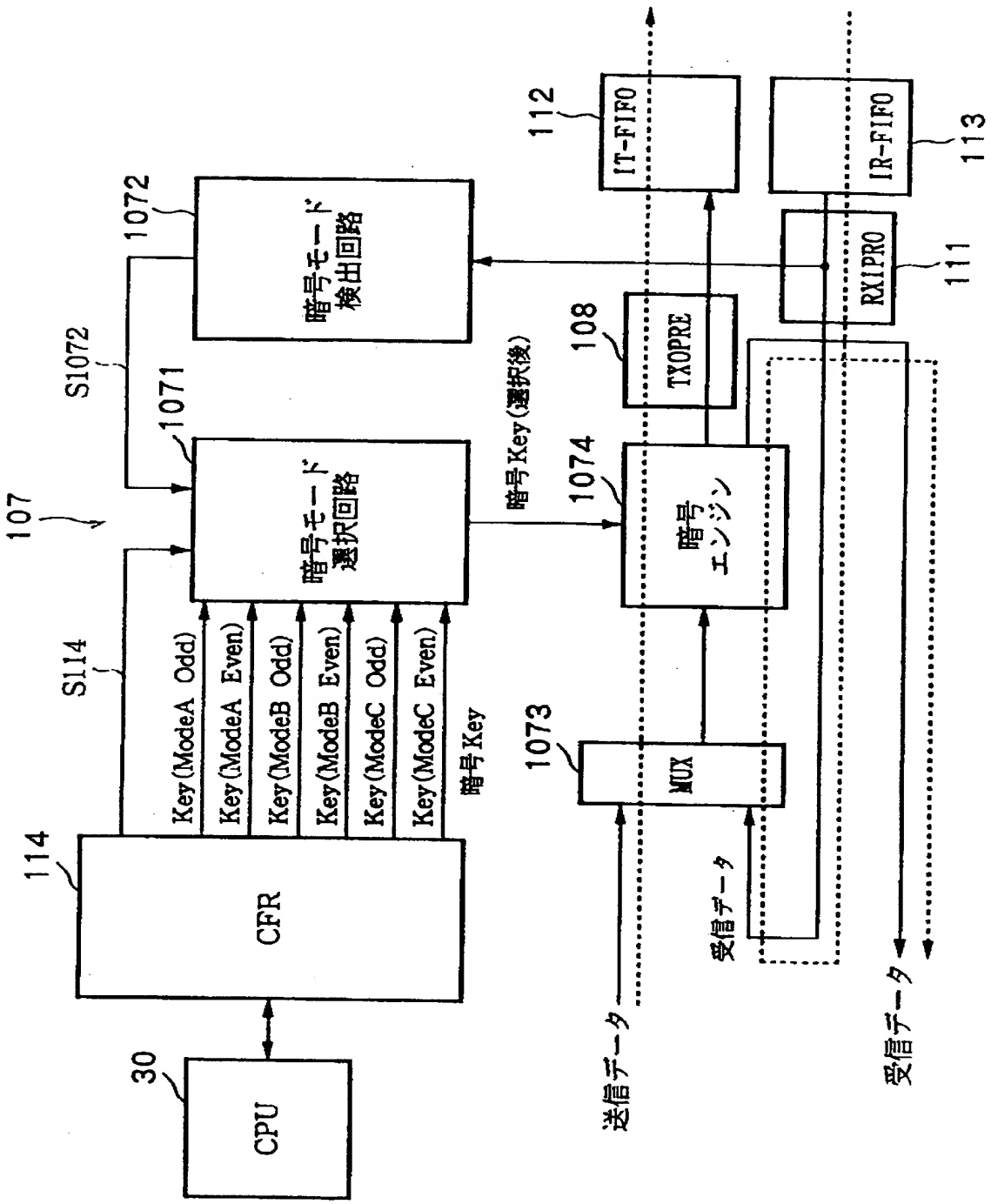
(A)

sy[3:2]	暗号モード	内 容
11	モードA	Never Copy
10	モードB	Copy Once
01	モードC	No More Copy
00	暗号化なし	Copy Free

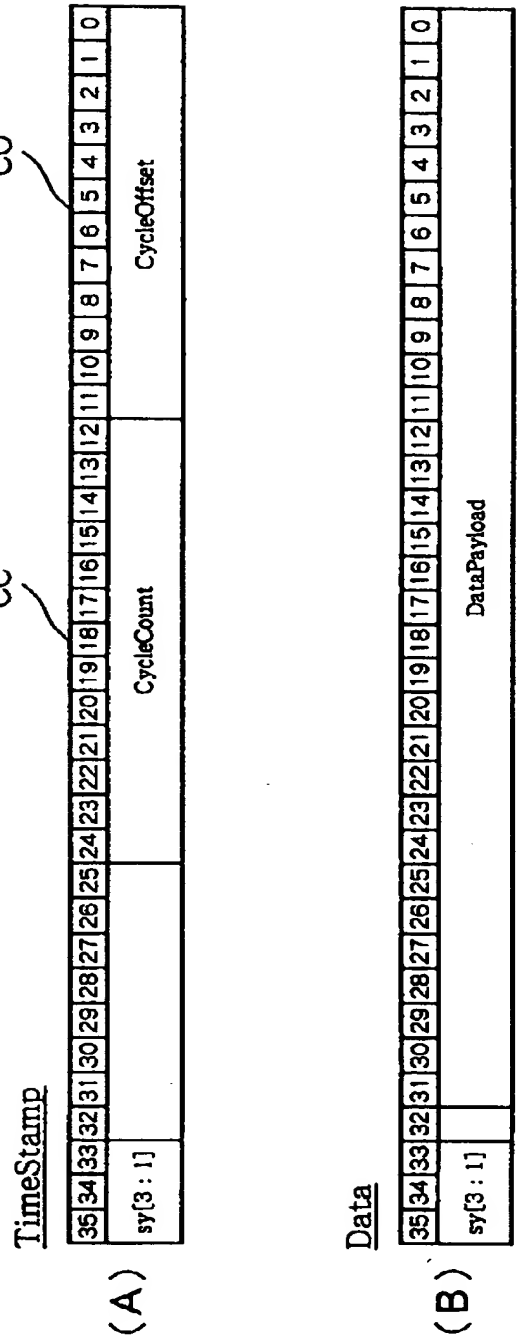
(B)

sy[1]	暗号 Key の種類
1	Even Key
0	Odd Key

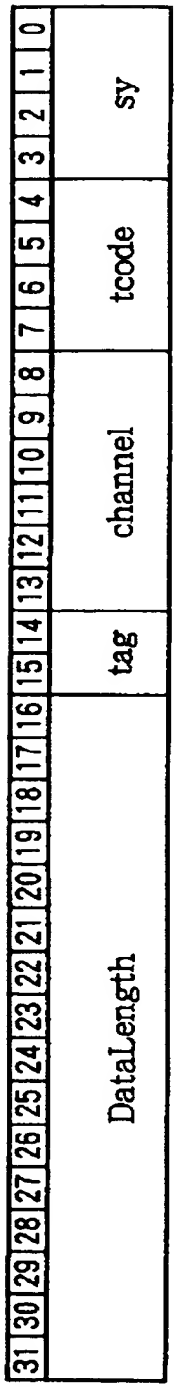
【図３】


CPU
30
CFR
114
S114
Key(ModeA Odd)
Key(ModeA Even)
Key(ModeB Odd)
Key(ModeB Even)
Key(ModeC Odd)
Key(ModeC Even)
暗号Key
107
暗号モード選択回路
1071
S1072
暗号モード検出回路
1072
暗号Key(選択後)
暗号エンジン
1074
MUX
1073
TXOPRE
108
RX1PRO
111
IT-FIFO
112
IR-FIFO
113
送信データ
受信データ
受信データ

【図４】

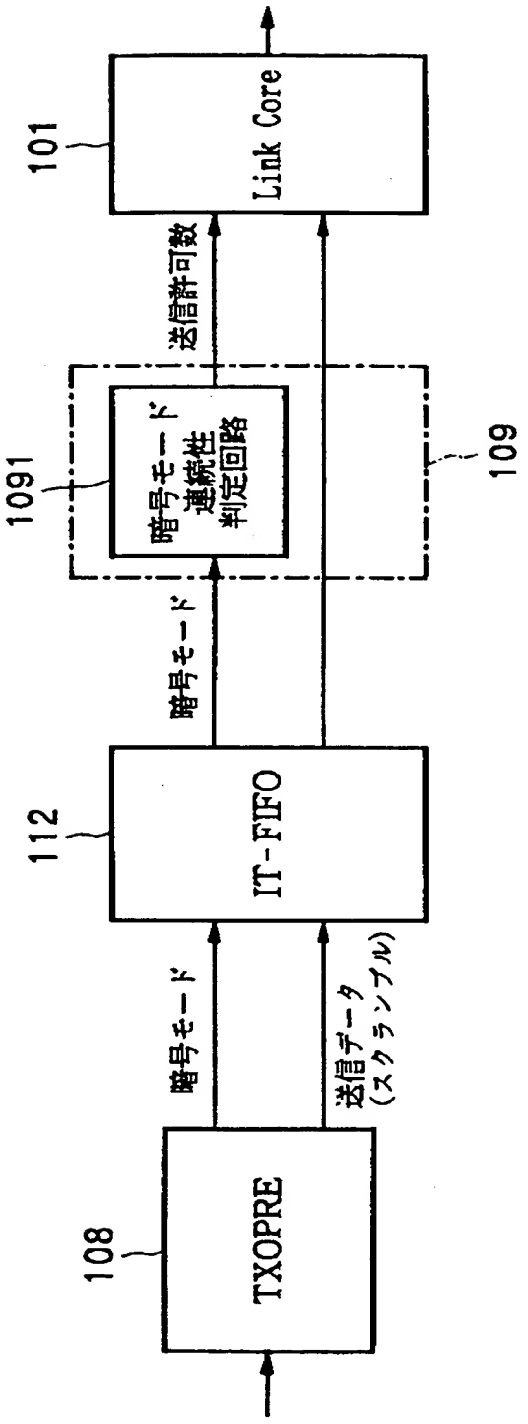

TimeStamp
(A)
CC
CO
35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
sy[3:1]
CycleCount
CycleOffset
Data
(B)
35 34 33 32 31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
sy[3:1]
DataPayload

【図５】

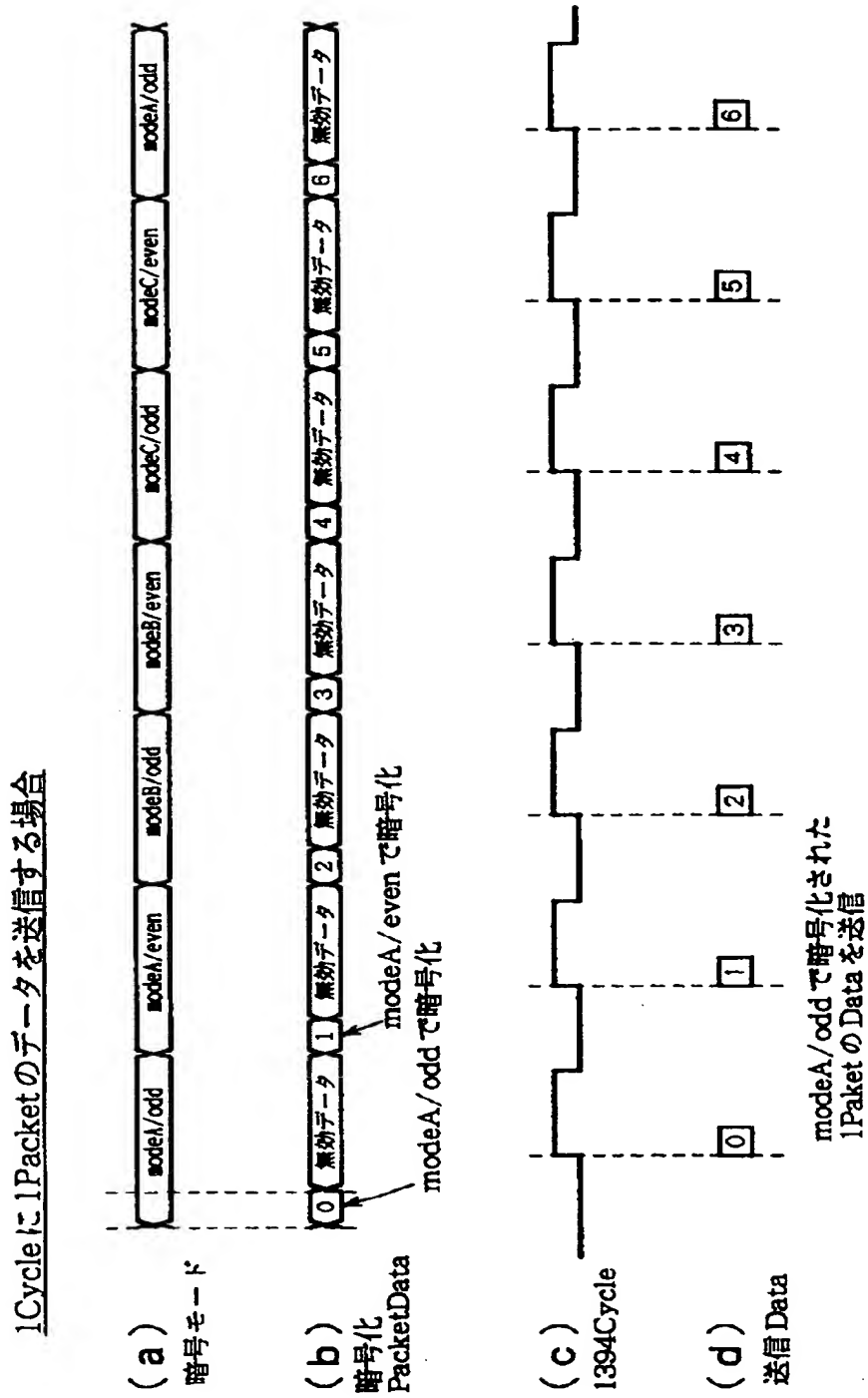


sy[3:0] のbit3-bit1を暗号モードに割り当てる。

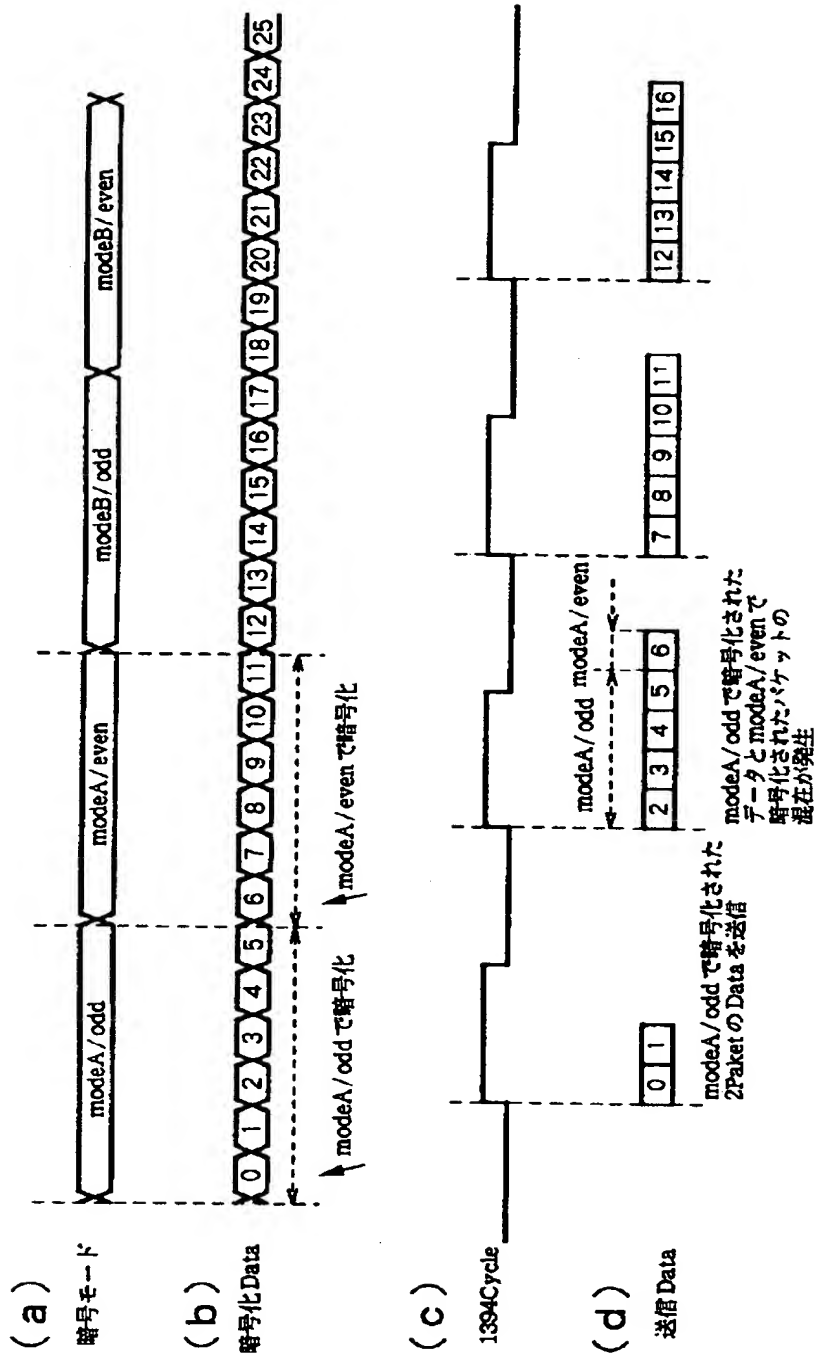
【図６】


101
Link Core
送信許可数
1091
暗号モード
通信性
判定回路
109
暗号モード
112
IT-FIFO
暗号モード
送信データ
(スクランブル)
108
TXOPRE

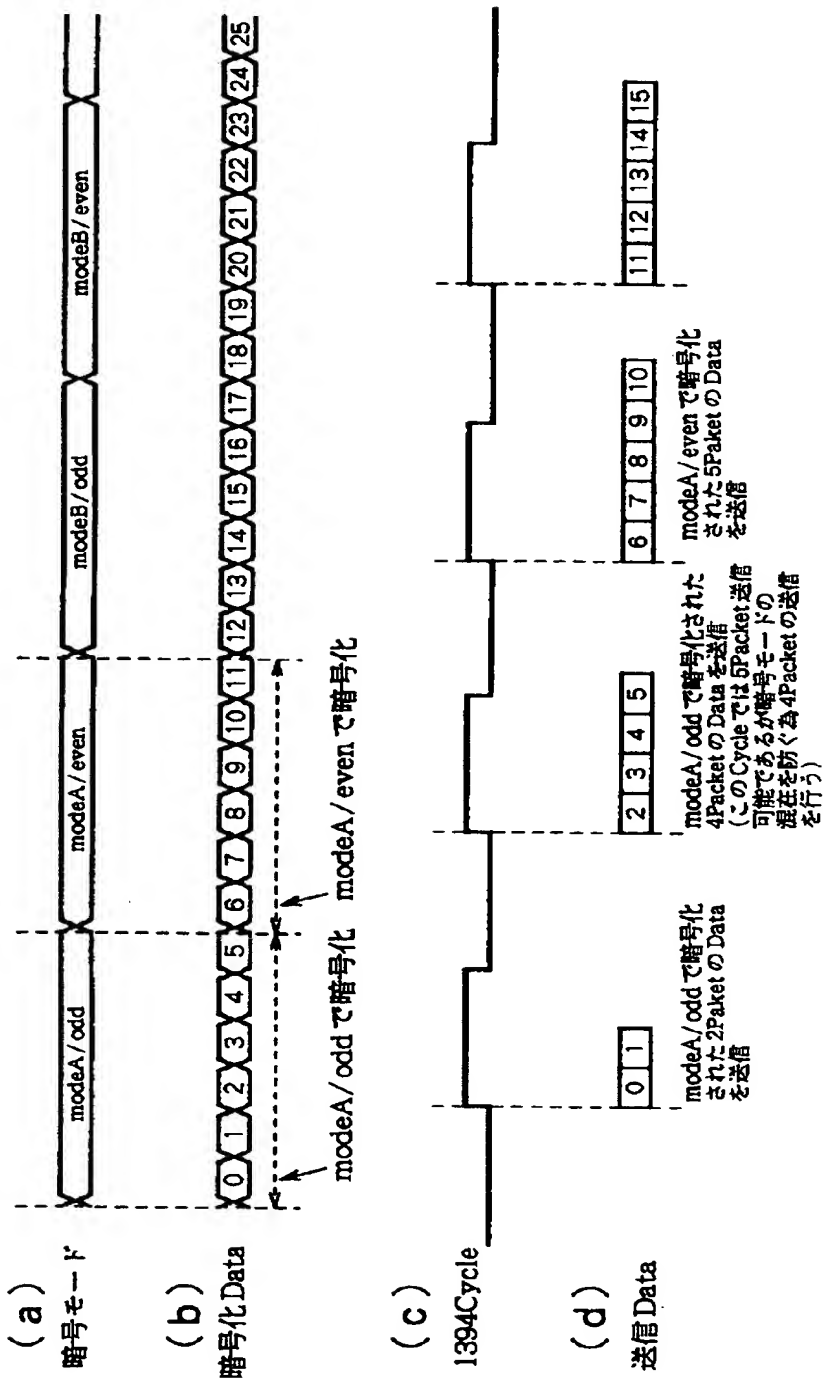
【図７】


1Cycle に 1Packet のデータを送信する場合
(a)
暗号モード
modeA/odd
modeA/even
modeB/odd
modeB/even
modeC/odd
modeC/even
modeA/odd
(b)
暗号化
PacketData
0
無効データ
1
無効データ
2
無効データ
3
無効データ
4
無効データ
5
無効データ
6
modeA/odd で暗号化
modeA/even で暗号化
(c)
1394Cycle
0
1
2
3
4
5
6
(d)
送信 Data
modeA/odd で暗号化された
1Paket の Data を送信

【図８】


(a)
暗号モード
modeA/odd
modeA/even
modeB/odd
modeB/even
(b)
暗号化Data
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
modeA/odd で暗号化
modeA/even で暗号化
(c)
1394Cycle
(d)
送信 Data
0 1
modeA/odd で暗号化された
2Paket の Data を送信
modeA/odd modeA/even
2 3 4 5 6
7 8 9 10 11
12 13 14 15 16
modeA/odd で暗号化された
データと modeA/even で
暗号化されたパケットの
衝突が発生

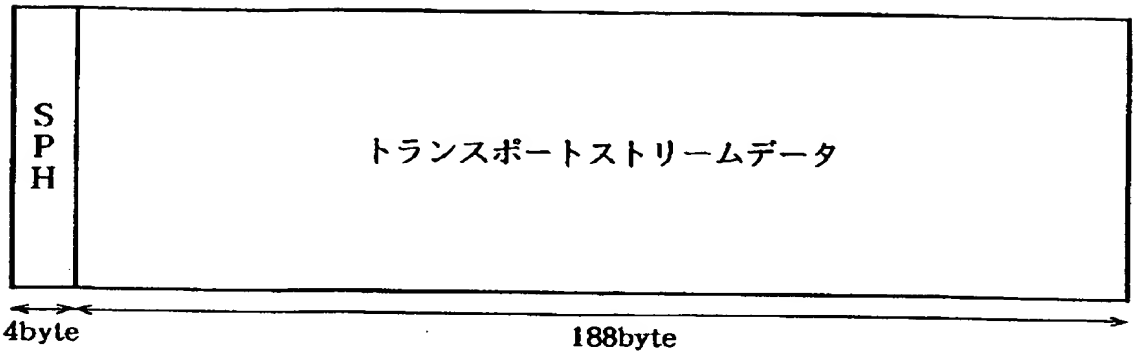
【図９】


(a)
暗号モード
modeA/odd
modeA/even
modeB/odd
modeB/even
(b)
暗号化Data
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
modeA/odd で暗号化
modeA/even で暗号化
(c)
1394Cycle
(d)
送信Data
0 1
modeA/odd で暗号化されたPacketのDataを送信
2 3 4 5
modeA/odd で暗号化されたPacketのDataを送信
(このCycleでは5Packet送信可能であるが暗号モードの混在を防ぐ為4Packetの送信を行う)
6 7 8 9 10
modeA/even で暗号化されたPaketのDataを送信
11 12 13 14 15

【図１０】

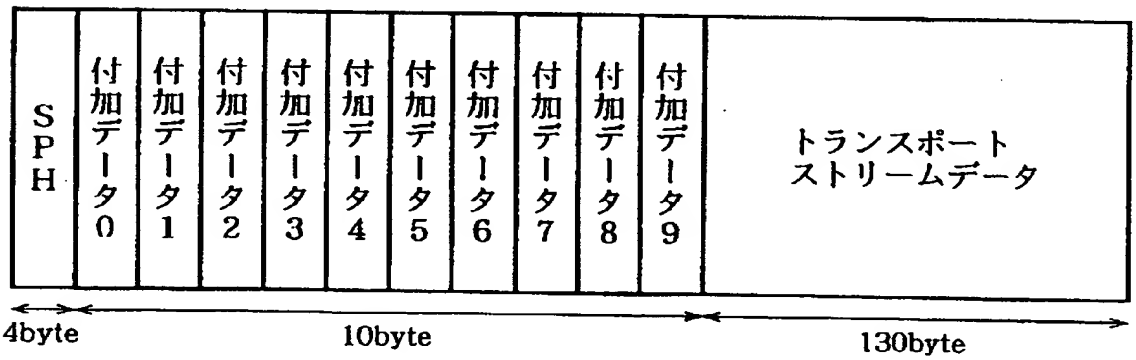
(A)

DVB

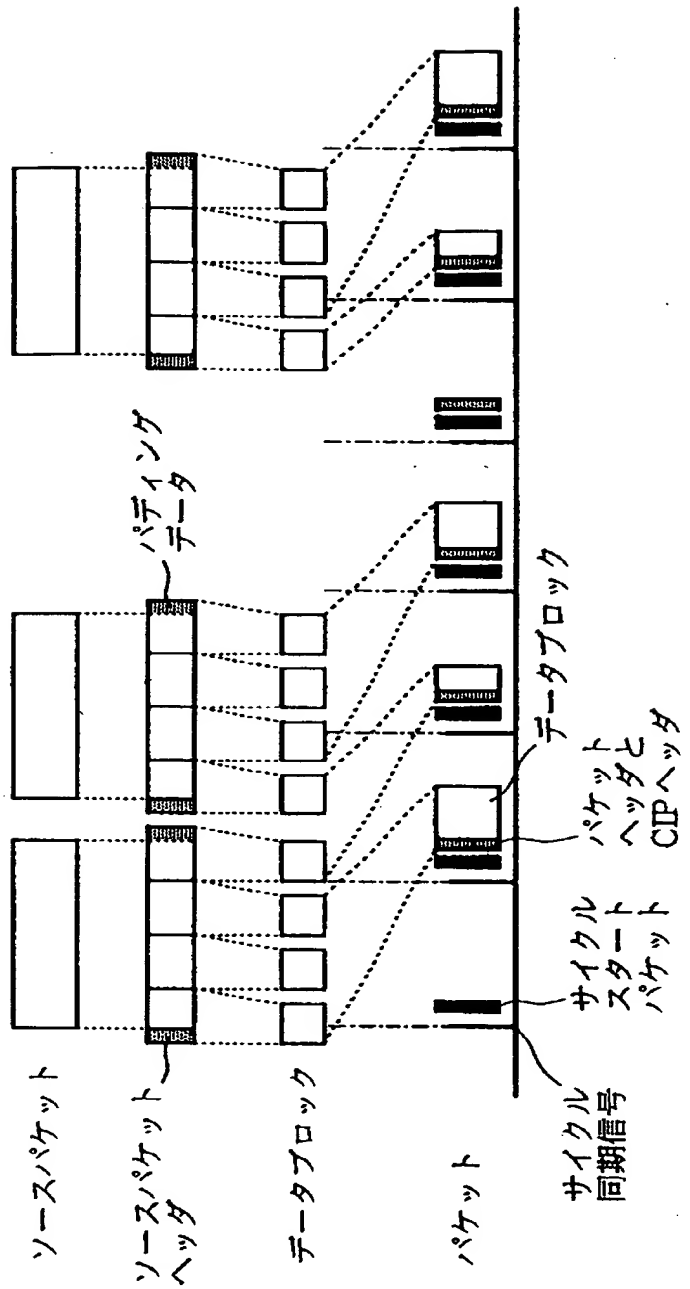


(B)

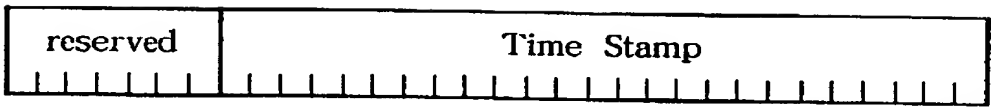
DSS



【図１１】

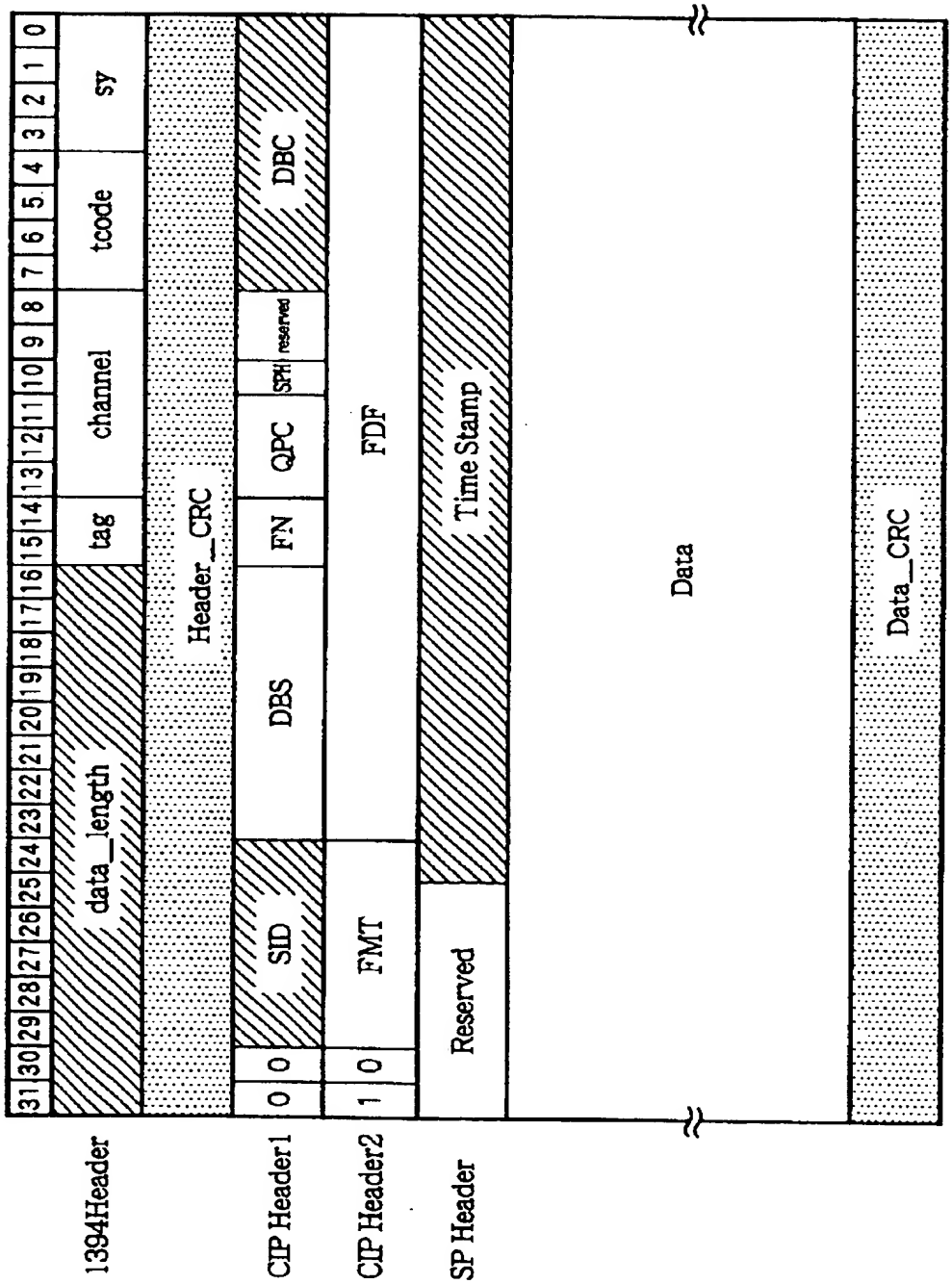

ソースパケット
ソースパケット
ヘッダ
パディング
データ
データブロック
パケット
サイクル
同期信号
サイクル
スタート
パケット
パケット
ヘッダと
CIPヘッダ
データブロック

【図１２】

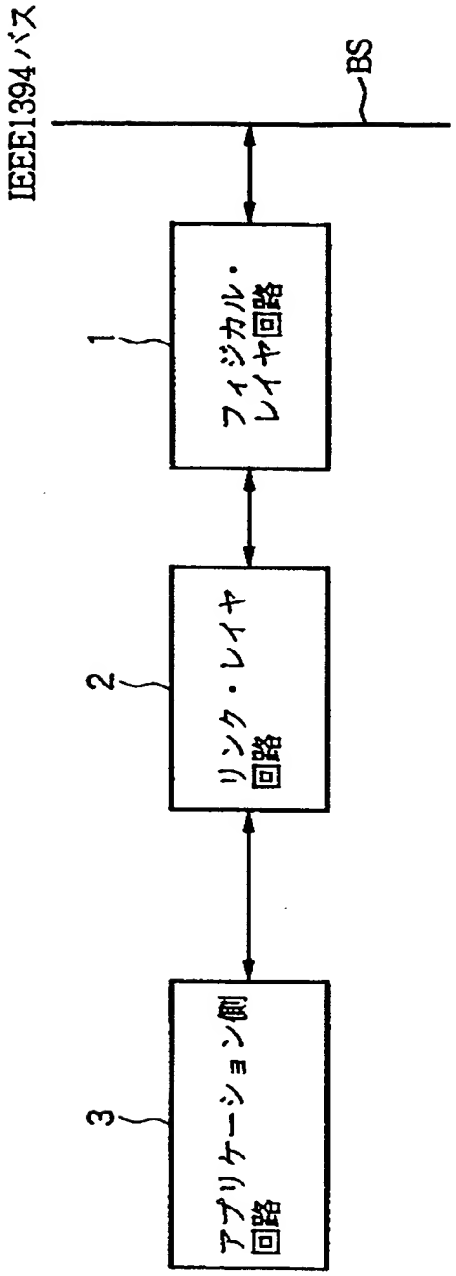


ソースパケットヘッダ (SPH)

【図１３】


31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
data_length
tag
channel
tcode
sy
Header_CRC
0 0
SID
DBS
FN
QPC
SPH
reserved
DBC
1 0
FMT
FDF
Reserved
Time Stamp
Data
Data_CRC
1394Header
CIP Header1
CIP Header2
SP Header

【図１４】



【書類名】　　要約書

【要約】

【課題】不正なコピーを防止しつつ、かつ複数の暗号モードを判別できず、復号できなくなることを防止でき、受信側において受信データを正しく復号することができる信号処理回路を提供する。

【解決手段】暗号モード連続性判定回路１０９１を設け、複数をパケットの送信時に、ＦＩＦＯ１１２から送信データを読み出した際に暗号モードの連続性を確認し、不連続性を確認したときは、その１３９４規格の送信サイクルで送信できる帯域に余裕があったとしても送信を停止させ、次のサイクルで異なる暗号キーで暗号化されたパケットを送信するように、リンクコア１０１の送信回路に指示して、１３９４規格の１サイクル内では、一つの暗号モードで暗号化されたデータのみを送信し、異なる暗号モードで暗号化されたデータは次のサイクルで送信するように構成する。

【選択図】　　図６

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000002185
【住所又は居所】　東京都品川区北品川６丁目７番３５号
【氏名又は名称】　ソニー株式会社
【代理人】　申請人
【識別番号】　100094053
【住所又は居所】　東京都台東区柳橋２丁目４番２号　創進国際特許事務所
【氏名又は名称】　佐藤　隆久

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社